

CLAIMS

What is claimed is:

- 1 1. An apparatus comprising:
2 a processor having a normal execution mode and a host execution mode;
3 and
4 a virtual machine monitor (VMM) operable in conjunction with the host
5 execution mode to create at least one protected mode environment to operate guest
6 software in a virtual machine;
7 wherein responsive to a command to switch between protected modes,
8 the VMM causes the processor to atomically switch between an original protected
9 mode environment and a target protected mode environment.
- 1 2. The apparatus of claim 1, wherein switching between protected modes
2 further includes entering a virtual machine execution (VMX) mode to enable virtual
3 machine functionality.
- 1 3. The apparatus of claim 1, further comprising a virtual machine control
2 structure (VMCS) to store state information for use in switching between the original
3 protected mode environment and the target protected mode environment, the VMCS to
4 store state information related to the original protected mode environment.
- 1 4. The apparatus of claim 3, wherein the virtual machine control structure
2 (VMCS) further stores state information related to the target protected mode
3 environment.
- 1 5. The apparatus of claim 4, wherein the virtual machine control structure
2 (VMCS) further stores a guest entry point field to point to a command used for
3 instructing the processor to exit out of the original protected mode environment and a
4 host entry point field to point to a command to instruct the processor to exit out of a
5 virtual machine execution (VMX) mode.
- 1 6. The apparatus of claim 1, wherein the VMM causes the processor to
2 enter a virtual machine execution (VMX) mode, to exit out of the original protected
3 mode environment, and to enter into the target protected mode environment.

1 7. The apparatus of claim 6, wherein the VMM causes the target protected
2 mode environment to exit out of the virtual machine (VMX) extension mode.

1 8. The apparatus of claim 7, wherein the processor resumes operation with
2 the target protected mode environment.

1 9. The apparatus of claim 1, wherein guest software operable in a protected
2 mode environment includes an operating system.

1 10. A method comprising:
2 providing a normal execution mode in a processor and a host execution
3 mode in a processor;
4 creating at least one protected mode environment to operate guest
5 software in a virtual machine; and
6 wherein responsive to a command to switch between protected modes,
7 atomically switching between an original protected mode environment and a target
8 protected mode environment.

1 11. The method of claim 10, wherein switching between protected modes
2 further includes entering a virtual machine execution (VMX) mode to enable virtual
3 machine functionality.

1 12. The method of claim 10, further comprising storing state information for
2 use in switching between the original protected mode environment and the target
3 protected mode environment including storing state information related to the original
4 protected mode environment.

1 13. The method of claim 12, further comprising storing state information
2 related to the target protected mode environment.

1 14. The method of claim 13, further comprising:
2 storing a guest entry point field to point to a command used for instructing the
3 processor to exit out of the original protected mode environment; and

4 storing a host entry point field to point to a command to instruct the processor to
5 exit out of a virtual machine execution (VMX) mode.

1 15. The method of claim 10, further comprising
2 entering a virtual machine execution (VMX) mode;
3 exiting out of the original protected mode environment; and
4 entering into the target protected mode environment.

1 16. The method of claim 15, further comprising exiting out of the virtual
2 machine (VMX) extension mode.

1 17. The method of claim 16, further comprising resuming operation with the
2 target protected mode environment.

1 18. The method of claim 10, wherein guest software operable in a protected
2 mode environment includes an operating system.

1 19. A machine-readable medium having stored thereon instructions, which
2 when executed by a machine, cause the machine to perform the following operations
3 comprising:
4 providing a normal execution mode in a processor and a host execution
5 mode in a processor;
6 creating at least one protected mode environment to operate guest
7 software in a virtual machine; and
8 wherein responsive to a command to switch between protected modes,
9 atomically switching between an original protected mode environment and a target
10 protected mode environment.

1 20. The machine-readable medium of claim 19, wherein switching between
2 protected modes further includes entering a virtual machine execution (VMX) mode to
3 enable virtual machine functionality.

1 21. The machine-readable medium of claim 21, further comprising storing
2 state information for use in switching between the original protected mode environment

3 and the target protected mode environment including storing state information related
4 to the original protected mode environment.

1 22. The machine-readable medium of claim 21, further comprising storing
2 state information related to the target protected mode environment.

1 23. The machine-readable medium of claim 22, further comprising:
2 storing a guest entry point field to point to a command used for instructing the
3 processor to exit out of the original protected mode environment; and
4 storing a host entry point field to point to a command to instruct the processor to
5 exit out of a virtual machine execution (VMX) mode.

1 24. The machine-readable medium of claim 19, further comprising
2 entering a virtual machine execution (VMX) mode;
3 exiting out of the original protected mode environment; and
4 entering into the target protected mode environment.

1 25. The machine-readable medium of claim 24, further comprising exiting
2 out of the virtual machine (VMX) extension mode.

1 26. The machine-readable medium of claim 25, further comprising resuming
2 operation with the target protected mode environment.

1 27. The machine-readable medium of claim 19, wherein guest software
2 operable in a protected mode environment includes an operating system.

1 28. A system comprising:
2 a processor including virtual machine extension (VMX) instruction
3 support, the processor further having a normal execution mode and a host execution
4 mode; and
5 a virtual machine monitor (VMM) operable in conjunction with the host
6 execution mode to create at least one protected mode environment to operate guest
7 software in a protected memory area;

8 wherein responsive to a command to switch between protected modes,
9 the VMM causes the processor to atomically switch between an original protected
10 mode environment and a target protected mode environment.

1 29. The system of claim 28, wherein switching between protected modes
2 further includes entering a virtual machine execution (VMX) mode to enable virtual
3 machine functionality.

1 30. The system of claim 28, further comprising a virtual machine control
2 structure (VMCS) to store state information for use in switching between the original
3 protected mode environment and the target protected mode environment, the VMCS to
4 store state information related to the original protected mode environment.

1 31. The system of claim 30, wherein the virtual machine control structure
2 (VMCS) further stores state information related to the target protected mode
3 environment.

1 32. The system of claim 31, wherein the virtual machine control structure
2 (VMCS) further stores a guest entry point field to point to a command used for
3 instructing the processor to exit out of the original protected mode environment and a
4 host entry point field to point to a command to instruct the processor to exit out of a
5 virtual machine execution (VMX) mode.

1 33. The system of claim 28, wherein the VMM causes the processor to enter
2 a virtual machine execution (VMX) mode, to exit out of the original protected mode
3 environment, and to enter into the target protected mode environment.

1 34. The system of claim 33, wherein the VMM causes the target protected
2 mode environment to exit out of the virtual machine (VMX) extension mode.

1 35. The system of claim 34, wherein the processor resumes operation with
2 the target protected mode environment.

1 36. The system of claim 28, wherein guest software operable in a protected
2 mode environment includes an operating system.